



HIPAA ADVANCED PRIVACY OFFICERS WORKSHOP FOR PROVIDERS

SEPTEMBER 4 AND 5, 2002

Ann Dirks-Linhorst, DMH Privacy
Officer

DISCLAIMER

(For Non-DMH Personnel)

- ▶ The Missouri Department of Mental Health does not give legal advice, nor allege any legal expertise. Information and advice provided should be accepted as general in nature to guide the DMH and its facilities' HIPAA Core Teams. Any and all other parties should consult professional counsel for specific legal advice.
- ▶ The information contained herein or otherwise presented in any format is compiled from official sources within and outside the MO DMH. The use of the enclosed materials is approved for compliance activities and other official business only, and is in no way intended to assert any guarantee of HIPAA compliance.
- ▶ Beyond the use as an educational resource only, any and all other use of the material is strictly prohibited. Any misappropriation or misuse of the materials should be reported immediately to Ann Dirks-Linhorst, MO DMH HIPAA Privacy Officer.

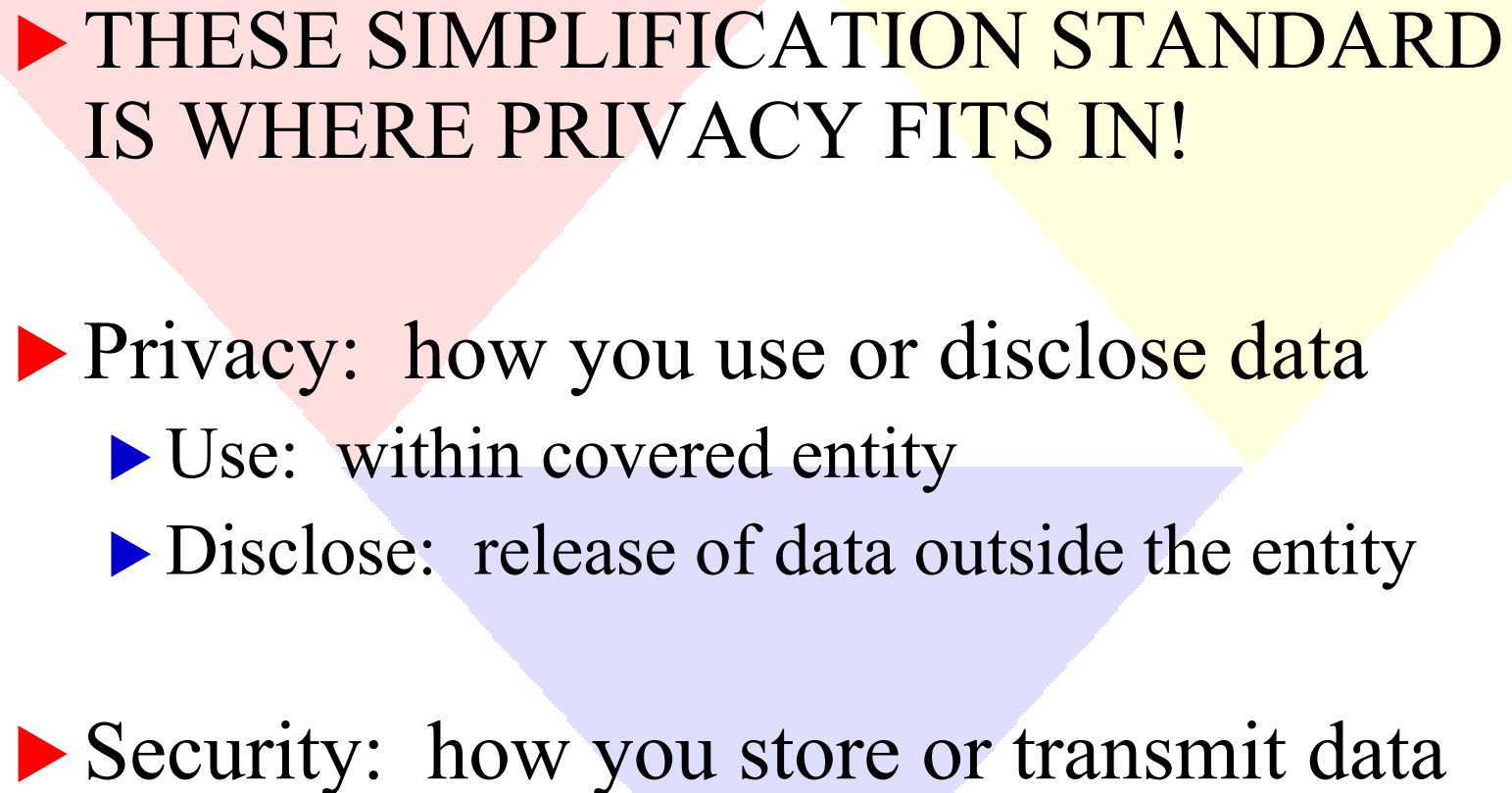
TODAY'S WORK SHOP GOALS

- ▶ Remember HIPAA basics.
- ▶ Identify why there is such hoopla over HIPAA.
- ▶ Answer the question: Is HIPAA really happening?
- ▶ Review Privacy Officer appointment.
- ▶ Discuss Selection of Privacy Assessment Tool
- ▶ Discuss specific HIPAA Privacy Rule requirements.
- ▶ Highlight proposed Privacy Rule modifications.
- ▶ Discuss HIPAA's Organized Health Care Arrangement.
- ▶ Answer frequently asked HIPAA Privacy questions.

HIPAA REMINDER

- ▶ Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191)
- ▶ Its purpose:
 - ▶ Expand fraud and abuse enforcement abilities
 - ▶ Provide for health insurance portability
 - ▶ Establish **Administrative Simplification Stds** to promote accountability to consumers of health care services

HIPAA REMINDER

- 
- ▶ THESE SIMPLIFICATION STANDARD IS WHERE PRIVACY FITS IN!
 - ▶ Privacy: how you use or disclose data
 - ▶ Use: within covered entity
 - ▶ Disclose: release of data outside the entity
 - ▶ Security: how you store or transmit data

WHY THE HOOPLA OVER HIPAA?



▶ CIVIL PENALTIES

- ▶ \$100 fine per person per violation
- ▶ \$25000 fine per year for multiple violations
- ▶ \$25000 fine cap per year per provision.

WHY THE HOOPLA OVER HIPAA?

▶ CRIMINAL PENALTIES

- ▶ Knowingly or wrongfully disclosing or receiving PHI: fine and/or one year prison time
- ▶ Commit offense under false pretenses: fine and/or five years prison time
- ▶ Intent to see PHI or client lists for personal gain or malicious harm: fine and/or ten years prison time.

WHY THE HOOPLA OVER HIPAA?

- ▶ Enforcement by Office of Civil Rights/Civil
- ▶ OCR may refer to Department of Justice/U.S. Attorney General's Office/Criminal
- ▶ Complaint can trigger OCR or OCR may conduct random compliance reviews

WHY THE HOOPLA OVER HIPAA?

- ▶ NPRM on enforcement expected anytime.
- ▶ Probable OCR enforcement strategy:
 - ▶ OCR provides technical assistance
 - ▶ OCR seeks agency cooperation and informal resolution, or
 - ▶ Covered entity may file compliance report/corrective action plan
 - ▶ Web site: www.hhs.gov/ocr/hipaa

IS HIPAA REALLY HAPPENING?

- ▶ Final Privacy Rule established April 2001.
- ▶ Modifications issued March 27, 2002.
- ▶ Modification accepted August 15, 2002.
- ▶ Current mandatory compliance date: April 14, 2003.
- ▶ Although President Bush signed one year extension for Transactions, the legislation specifically exempted Privacy from the extension.
- ▶ Supported by both Clinton and Bush administrations.
- ▶ May or may not have legislative extension requests.

IS HIPAA REALLY HAPPENING?

▶ DMH'S APPROACH:

- ▶ Assume we need to assure compliance by **April 14, 2003**, until told otherwise.
- ▶ All HIPAA requirements will be set forth in Department Operating Regulation for consistency among all state-operated.
- ▶ DMH will review Code of State Regulations for changes to Licensing & Certification, etc.

DMH HIPAA APPROACH

- ▶ HIPAA is an organizational-wide issue – not just IT
- ▶ Will require re-tooling of IT, but also development and promulgation of policies and procedures
- ▶ There is no quick fix, out of the box solution to meet HIPAA requirements (CIMOR can assist with Transactions and Code Sets, but will NOT assure HIPAA Privacy compliance).

DOES HIPAA COVER ME?

- ▶ Key term is Covered Entity
 - ▶ Health plans – and their business partners
 - ▶ Health care clearinghouses
 - ▶ Health care providers who transmit health information in electronic form – and their business associates
 - ▶ Small health plans have until April 14, 2004, for compliance efforts.

DOES HIPAA COVER ME?

- ▶ Applies to protected health information (PHI) **in any form** – paper, electronic and oral communications.
- ▶ Does not apply to information that has been de-identified
- ▶ Does **not** require “consent” BUT **will require** “authorization”
- ▶ Health advocates and professional groups (AHIMA, etc.) strongly support Privacy Rule
- ▶ Assessment Tool online at DMH Web Page

HIPAA REQUIRES.....

- ▶ Policies and procedures to protect PHI
- ▶ Designate a Privacy Officer
- ▶ Requires Privacy Training
- ▶ Establish Sanctions or Penalties policy
- ▶ Establish a number of specific client rights

▶ *Now, let's talk more about each specific requirement*

HIPAA REQUIRES.....

- ▶ Designation of Privacy Officer
 - ▶ Each covered entity must designate a Privacy Officer
 - ▶ The Rule does not require that the person be from any specific discipline
 - ▶ DMH established draft facility privacy officer duties (Appendix A)
 - ▶ DMH redirected internal resources for all privacy officer functions.

PRIVACY OFFICER: FIRST PROJECT

- ▶ Select and Implement a Privacy Assessment Tool
 - ▶ DMH looked to MO SNIP/Other states for potential work product
 - ▶ Selected one assessment tool/enhanced for DMH (Appendix B)
 - ▶ Conducted mandatory training with privacy officers on assessment tool
 - ▶ Worked with OIS to develop on-line application of tool
 - ▶ Conducted pilot of tool, and then took it statewide
 - ▶ Completed assessment in one month
 - ▶ Reviewed data for gap implications

SO WHAT IF I FIND GAPS?

- ▶ Compare HIPAA Privacy Rule standards to current business practices
- ▶ Any place current practices fall short of HIPAA Privacy standards constitutes a gap
- ▶ Identify all gaps
- ▶ Formulate corresponding work plan or list of deliverables (Appendix C).
- ▶ That work plan should include all HIPAA standards, such as

HIPAA REQUIRES.....

- ▶ Identify Protected Health Information (PHI)
 - ▶ Individually identifiable health information
 - ▶ Written, oral, electronic
 - ▶ Who is asked for PHI in your organization; at how many levels; where do those requests come from; and can you identify routine sources to whom you disclose PHI
 - ▶ If you do not know where PHI is, and who asks for it, protecting it will be difficult.

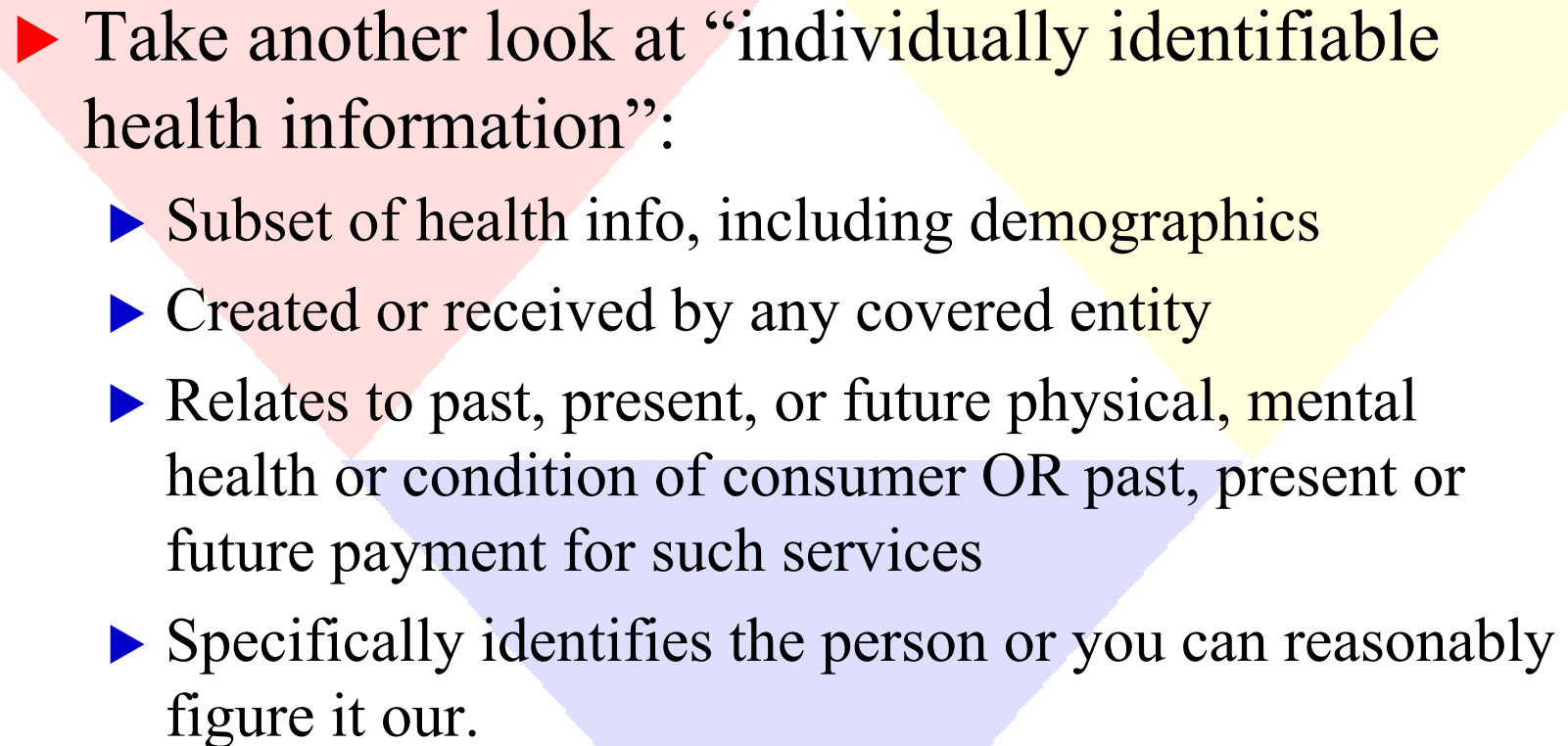
HIPAA REQUIRES.....

- ▶ Exclusions from PHI:
 - ▶ Education records covered by FERPA
 - ▶ Health information maintained in employer's health records (proposed)
 - ▶ Psychotherapy notes: notes by mental health professionals documenting or analyzing contents of conversation during private, group, joint or family counseling AND that are maintained separately from the rest of the medical record

HIPAA REQUIRES.....

- ▶ Applies to records in a “designated records set” (Section 164.501)
 - ▶ A group of records consisting of:
 - ▶ Medical records and billing records
 - ▶ Enrollment, payment, claims adjudication, case or medical management records, or
 - ▶ Used, in whole or in part, by or for the covered entity, to make decisions about consumers.

HIPAA REQUIRES....

- 
- ▶ Take another look at “individually identifiable health information”:
 - ▶ Subset of health info, including demographics
 - ▶ Created or received by any covered entity
 - ▶ Relates to past, present, or future physical, mental health or condition of consumer OR past, present or future payment for such services
 - ▶ Specifically identifies the person or you can reasonably figure it out.

HIPAA REQUIRES....

- ▶ Consent (NOT required by final Rule)
 - ▶ Consent was mandatory under final Privacy Rule, but removed in modifications
 - ▶ Covered entity still allowed the option of obtaining consent for use/disclosure of PHI for treatment, payment, and health care operations
 - ▶ DMH anticipates standardizing consent for use across all three divisions
 - ▶ DMH will continue to obtain consent for treatment

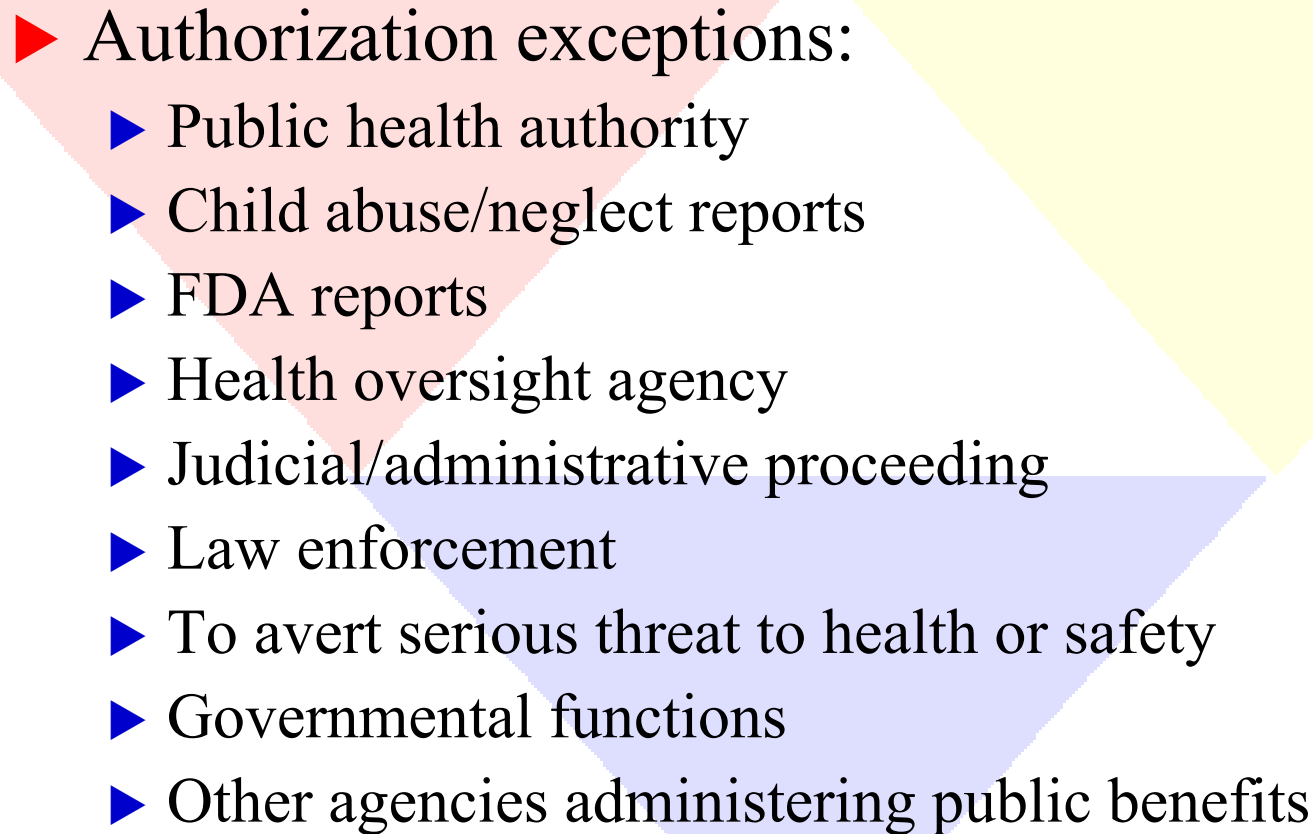
HIPAA REQUIRES.....



▶ Authorization

- ▶ Required to disclose PHI to a specific third party
- ▶ Must be specific as to what PHI is to be shared with whom and for what purpose
- ▶ Must also contain revocation language
- ▶ Cannot condition treatment on signing an authorization

HIPAA REQUIRES....

- 
- ▶ Authorization exceptions:
 - ▶ Public health authority
 - ▶ Child abuse/neglect reports
 - ▶ FDA reports
 - ▶ Health oversight agency
 - ▶ Judicial/administrative proceeding
 - ▶ Law enforcement
 - ▶ To avert serious threat to health or safety
 - ▶ Governmental functions
 - ▶ Other agencies administering public benefits

HIPAA REQUIRES.....

- ▶ Notice of Privacy Practices (NPP)
 - ▶ Purpose: provide consumer with adequate notice of uses or disclosures of PHI
 - ▶ Must be written in plain language
 - ▶ Rule lists examples of types of uses to include in the NPP

HIPAA REQUIRES....

▶ NPP continued:

- ▶ Final Rule requires that covered entity make good faith effort to have consumer “acknowledge” receipt of NPP
- ▶ Requires that NPP will be posted on premises
- ▶ Must include NPP on any web site that covered entity maintains
- ▶ Separate covered entities may have joint notice.

HIPAA REQUIRES CONSUMER RIGHTS PROVISIONS

► **Restrictions**

- ▶ Consumers may request the covered entity restrict how it uses/discloses PHI
- ▶ Covered entity NOT required to accept
- ▶ If restriction accepted, then covered entity must follow that restriction
- ▶ An exception exists for using or disclosing PHI for emergency treatment purposes

HIPAA REQUIRES CONSUMER RIGHTS PROVISIONS

▶ Access

- ▶ Under HIPAA consumers have the ability to access (defined as to inspect and copy) PHI in a designated records set
- ▶ If request is denied, the reason will determine whether or not there is a right of review
- ▶ Denial **without** right of review includes PHI from correctional institution; research; or if information was obtained by someone other than provider.

HIPAA REQUIRES CONSUMER RIGHTS PROVISIONS

▶ **Access continued:**

- ▶ Denial **with** right of review includes: if access is reasonably likely to endanger life or physical safety of self or others, whether staff or someone else; or request made by personal representative and access may cause harm to consumer or other person.
- ▶ Review is by licensed health care professional.

HIPAA REQUIRES CONSUMER RIGHTS PROVISIONS

▶ **Access continued:**

- ▶ Covered entity must act on written request within 30 days (entity may require that the request be in writing)
- ▶ If information not on site, may have up to 60 days to act on request.
- ▶ Covered entity may request additional 30 days but must do so in writing and stating reason for such delay.
- ▶ Covered entity may charge for copies.
- ▶ **KEEP DOCUMENTATION OF ALL DECISIONS!**

HIPAA REQUIRES CONSUMER RIGHTS PROVISIONS

▶ **Amendment**

- ▶ Covered entity has 60 days to act on consumer's request to amend PHI in designated records set
- ▶ Entity may deny request if:
 - ▶ PHI not created by entity
 - ▶ PHI not part of the designated records set
 - ▶ PHI not available under the access provisions
 - ▶ PHI is accurate and complete.

HIPAA REQUIRES CONSUMER RIGHTS PROVISIONS

▶ **Amendment continued:**

- ▶ If granted, make the amendment, and attempt to get the amended information to those who may have relied on past information to detriment of consumer
- ▶ If denied, advise in writing.
- ▶ Consumer can then give written statement disagreeing with denial.
- ▶ Covered entity must include the denial, and any written statement of disagreement, with any subsequent disclosure of that PHI.

HIPAA REQUIRES CONSUMER RIGHTS PROVISIONS

▶ **Accounting of Disclosures**

- ▶ Consumers have right to an accounting of disclosures for **six years** starting 4.14.2003.
- ▶ DMH approach
- ▶ Exceptions:
 - ▶ Disclosures for treatment, payment, HCO
 - ▶ Disclosures to consumers of own PHI
 - ▶ National security/intelligence purposes
 - ▶ Law enforcement

HIPAA REQUIRES CONSUMER RIGHTS PROVISIONS

▶ **Accounting of Disclosures cont'd:**

▶ Accounting must include:

- ▶ Date
- ▶ To whom and address
- ▶ Brief description of PHI disclosed
- ▶ Purpose of disclosure
- ▶ Must be given no later than 60 days after receipt
- ▶ May have one time 30 day extension
- ▶ One free request within 12 month period, then reasonable cost based approach for charging
- ▶ **KEEP DOCUMENTATION!!!**

HIPAA REQUIRES CONSUMER RIGHTS PROVISIONS

- ▶ Covered Entity must adhere to “minimum necessary” standard
 - ▶ Must provide only PHI in the minimum necessary amount to accomplish the purpose for which use or disclosure is sought
 - ▶ Minimum necessary does not apply when consumer executes valid authorization
 - ▶ Covered entity may set criteria for minimum necessary standard for routine PHI requests.

WHAT ELSE DOES HIPAA REQUIRE?

▶ **Training:**

- ▶ Entire workforce as necessary and appropriate for the workforce members to carry out function within the covered entity.
- ▶ Completed **prior** to April 14, 2003.
- ▶ DMH work plan for training efforts.
- ▶ Training on three occasions:
 - ▶ Initial
 - ▶ New employee orientation
 - ▶ When material change made to policies or procedures affecting that workforce member.

WHAT ELSE DOES HIPAA REQUIRE?



▶ **Sanctions or Penalties**

- ▶ Covered entity must have policy for those who fail to comply with Privacy requirements
- ▶ Must document that sanctions **were** applied

WHAT ELSE DOES HIPAA REQUIRE?

▶ **Verification**

- ▶ Covered entity must verify that the person or entity requesting PHI is who they represent themselves to be.
- ▶ Must document that covered entity has done so.
- ▶ DMH approach is web based application, designed in conjunction with accounting of disclosures requirement.

WHAT ELSE DOES HIPAA REQUIRE?

▶ **Preemption of state law**

- ▶ Privacy Rule preempts any other state law **unless** that state law is more stringent (i.e. provides more protection for the consumer)
- ▶ Example: Section 630.140, RSMo
- ▶ HHS can grant an exception to preemption if the state law is necessary for health care administration, needed for public health or to regulate controlled substances, or if it is related to certain reporting requirements

WHAT ELSE DOES HIPAA REQUIRE?

- ▶ Health information must be **de-identified**
- ▶ Can be de-identified either by using a statistical methodology to assure no significant likelihood of identification, OR
- ▶ Final Privacy Rule creates a limited dataset for researches and those involved with public health studies.
 - ▶ Leave dates/geographic areas/admission-discharge dates/date of death
 - ▶ But, need to have data use agreement in place.

WHAT ELSE DOES HIPAA REQUIRE?

▶ **De-identification cont'd:**

▶ **Must remove:**

- ▶ Names
- ▶ Geographic subdivisions smaller than a state
- ▶ All dates, except year, of birth, admission, etc.
- ▶ Telephone, fax, or e-mail information
- ▶ SSN, medical records number, health plan number, certificates, etc.
- ▶ Finger, voice prints, photograph
- ▶ Any other identifiable characteristic

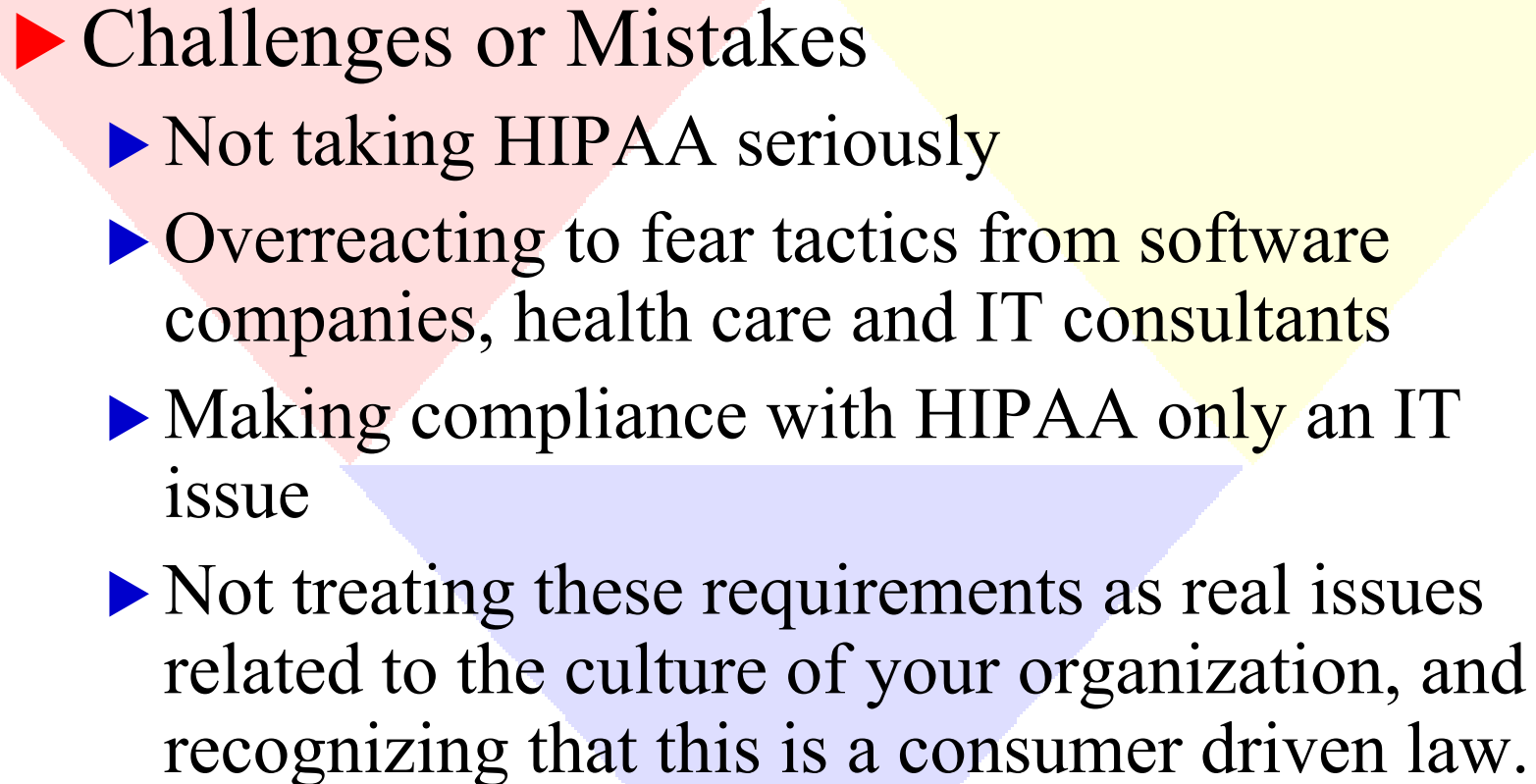
HIPAA IMPLEMENTATION

- ▶ DMH and its contract providers may participate in what HIPAA terms a “**organized health care arrangement**”
- ▶ Defined in Section 164.501 in HIPAA
- ▶ Clinically integrated care setting where consumers receive health care from more than one health care provider
- ▶ Includes more than one covered entity which holds themselves out as participating in joint arrangement
- ▶ Participate together in utilization review, or quality assessment and improvement activities; or PHI is shared between the two entities for purposes of financial risk determinations.

HIPAA IMPLEMENTATION

- ▶ Missouri statutes support such a joint arrangement (see Sections 632.050; 630.407; 631.010; 631.025; 633.010; and 633.025, RSMO, all speaking to DMH contracting for consortium or continuum of mental health care in the community)
- ▶ Such an **organized health care arrangement** fits with the purpose of CIMOR

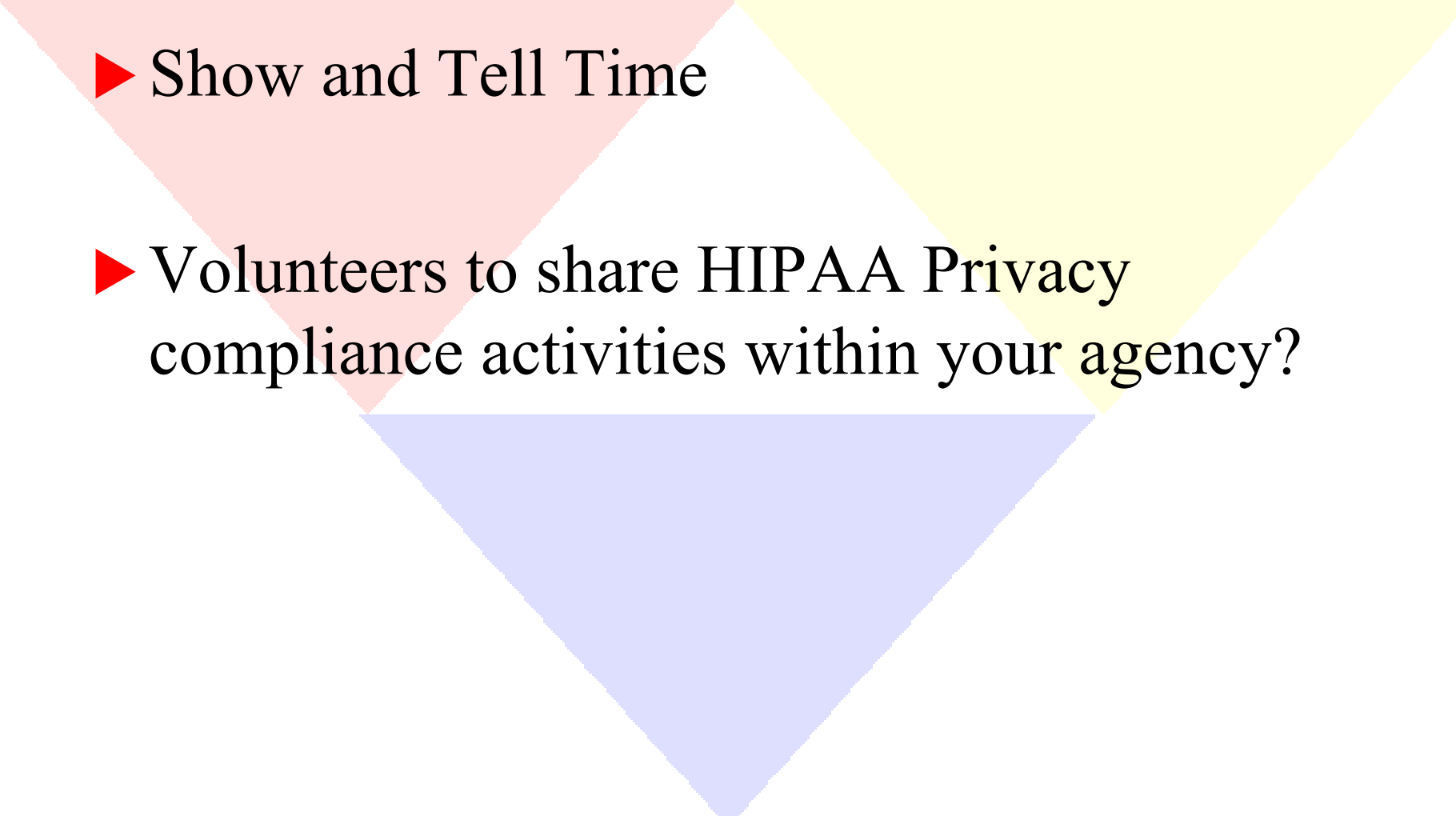
HIPAA IMPLEMENTATION

- 
- ▶ Challenges or Mistakes
 - ▶ Not taking HIPAA seriously
 - ▶ Overreacting to fear tactics from software companies, health care and IT consultants
 - ▶ Making compliance with HIPAA only an IT issue
 - ▶ Not treating these requirements as real issues related to the culture of your organization, and recognizing that this is a consumer driven law.

HIPAA IMPLEMENTATION

- ▶ Accepted Modifications to Privacy Rule adopted August 15, 2002
 - ▶ Removes mandatory consent requirement
 - ▶ Allowed to leave in a set of previously considered de-identified variable requirements
 - ▶ Allows extension of time for business associates contractual language (one more year)
 - ▶ Allows some uses of PHI for marketing.

HIPAA IMPLEMENTATION

- 
- ▶ Show and Tell Time
 - ▶ Volunteers to share HIPAA Privacy compliance activities within your agency?

HIPAA IMPLEMENTATION

▶ Helpful web-sites

- ▶ <http://aspe.hhs.gov/admsimp>
- ▶ <http://www.ahima.org>
- ▶ <http://www.hipaadvisory.com/>
- ▶ www.privacyassociation.org
- ▶ Mental Health HIPAA List Serve Group,
www.groups.yahoo.com/group/mh-hipaa
- ▶ www.jnci.com/mosnip
- ▶ www.modmh.state.mo.us/homeinfo/hipaa/index.htm

APPENDIX

- ▶ Appendix A: Suggested Facility Privacy Officer Job Duties
- ▶ Appendix B: HIPAA Privacy Assessment Tool
- ▶ Appendix C: MO DMH HIPAA Privacy Deliverables